UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION
CIVIL CASE NO.: 3:24-cv-00811

SEBESTIAN OWENS, ROBERT HAMILTON, and JEFFREY CRAIG, o*n behalf of themselves and all others similarly situated,* Plaintiffs, v. ALLY FINANCIAL INC., and ALLY BANK, Defendants.	**CLASS ACTION** **JURY TRIAL DEMANDED**

CONSOLIDATED AMENDED
CLASS ACTION COMPLAINT

Plaintiffs Sebestian Owens, Robert Hamilton, and Jeffrey Craig ("Plaintiffs"), as individuals and on behalf of all others similarly situated, bring this Class Action Complaint ("Complaint") against Defendants Ally Financial Inc. and Ally Bank (collectively, "Ally" or "Defendant") and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the data breach wherein an unauthorized actor accessed Ally's computer systems and that Ally discovered on or about July 17, 2024 (the "Data Breach").[1]

[1] *See* Notice Letter, available at https://www.mass.gov/doc/assigned-data-breach-number-2024-1004-ally-bank/download.

2. Defendant Ally Financial Inc. is a financial holding company that, through its subsidiaries including Defendant Ally Bank, offers online-only banking, credit card, investing, and home and auto loan services.[2]

3. Plaintiffs bring this Complaint against Ally for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its customer relationship with Plaintiffs and Class Members. Upon information and belief, such sensitive information includes, but is not limited to, Plaintiffs' and Class Members' (defined below) names and Social Security numbers (collectively defined herein as "PII").

4. Defendant received Plaintiffs' and Class Members' PII as a condition of entering into financial services with Ally. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Ally assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. In addition, Plaintiffs' and Class Members' highly sensitive personal information—which was entrusted to Defendant—was compromised and unlawfully accessed and extracted during the Data Breach despite Defendant's affirmative promise that it "maintain[ed] administrative, technical, and physical safeguards designed to protect your personal information."[3]

6. According to the letter that Ally sent to Plaintiffs and Class Members, Ally admits an unauthorized actor unlawfully accessed certain personal information from its network.

7. The Data Breach was a direct result of Ally's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' PII.

[2] https://www.ally.com/about/company-structure/(last accessed September 20, 2024).
[3] https://www.ally.com/about/ (last accessed September 20, 2024).

8. The mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Ally, and thus Ally was on notice that failing to take steps necessary to secure PII from those risks left that property in a dangerous condition.

9. Defendant breached its duties and obligations in one or more of the following ways: (1) by failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) by failing to design, implement, and maintain reasonable data retention policies; (3) by failing to adequately train staff on data security; (4) by failing to comply with industry-standard data security practices; (5) by failing to warn Plaintiffs and Class Members of Ally's inadequate data security practices; (6) by failing to encrypt or adequately encrypt the PII; (7) by failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) by failing to utilize widely available software able to detect and prevent this type of attack, and (9) by otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

10. Plaintiffs' and Class Members' identities are now at risk because of Ally's negligent conduct since the PII that Ally collected and maintained is now in the hands of data thieves.

11. As a result of the Data Breach, Plaintiffs and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiffs and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft. As a result of Ally's unreasonable and inadequate data security practices, Plaintiffs and Class Members have suffered numerous actual and concrete injuries and damages.

12. Plaintiffs and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

13. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity while mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of their PII; and (f) the continued risk to their sensitive PII, which remains in the possession of Ally, and which is subject to further breaches, so long as Ally fails to undertake appropriate and adequate measures to protect it collected and maintained.

14. The exposure of one's PII to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiffs' and the Class's PII was exactly that: private. Not anymore. Now, their PII is forever exposed and unsecure.

II. PARTIES

15. Plaintiff Sebestian Owens is a natural person, resident and citizen of the state of South Carolina.

16. Plaintiff Robert Hamilton is a natural person, resident and citizen of the state of Texas.

17. Plaintiff Jeffrey Craig is a natural person, resident and citizen of the state of Arizona.

18. Defendant Ally Financial Inc. is a Delaware corporation with its headquarters and principal place of business located at 601 S. Tyron Street, Charlotte, North Carolina 28202.

19. Defendant Ally Bank is a Delaware corporation with its headquarters and principal place of business located at 601 S. Tyron Street, Charlotte, North Carolina 28202.

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiffs, are citizens of a state different from Defendants.

21. This Court has personal jurisdiction over Defendants because their principal places of business are in this District.

22. Venue is proper under 18 U.S.C. § 1391(b)(1) because Defendants' principal places of business are in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

IV. FACTUAL BACKGROUND

Defendant's Business

23. Ally offers online-only financial services, including banking (checking accounts, savings accounts, etc.).

24. Upon information and belief, Plaintiffs and Class Members are current and former customers of Ally who entrusted their PII with Ally as a condition of receiving services.

25. The information held by Ally in its computer systems included the unencrypted PII of Plaintiffs and Class Members.

26. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Ally to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

27. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties. Ally has a legal duty to keep consumer's PII safe and confidential.

28. Defendant had obligations created by FTC Act, contract, industry standards, and upon information and belief, representations made to its customers and thereby Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

29. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Ally could not conduct its business.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Ally assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

The Data Breach

31. According to the Notice Letter dated May 23, 2024, made available by the Attorney General of Massachusetts, Ally admits that it became aware on April 23, 2024, that customers' "personal information may have been accessed by an unauthorized party who gained access to a

vendor's systems."[4] Ally admits that the information exposed includes Social Security numbers, dates of birth, and auto account numbers.[5]

32. Furthermore, upon information and belief, the PII was published, offered for sale and sold on the dark web by cybercriminals, which is the modus operandi of cybercriminals of this type.

33. Clearly, Ally failed to adequately protect Plaintiffs' and Class Members' PII—and failed to even encrypt or redact this highly sensitive PII. This unencrypted, unredacted PII was compromised, published, and then sold on the dark web, due to Ally's negligent and/or careless acts and omissions and their utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

34. Defendant has failed to provide Plaintiffs and Class Members with timely and adequate notice including, but not limited to, information about how the Data Breach occurred and even when it occurred and when Plaintiffs' and Class Members' information was released onto the dark web.

Data Breaches Are Preventable.

35. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[6]

---

[4] *See* https://www.mass.gov/doc/assigned-data-breach-number-2024-1004-ally-bank/download.
[5] *Id*.
[6] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Sept. 4, 2024).

36. To prevent and detect cyber-attacks and/or ransomware attacks Ally could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[7]

37. To prevent and detect cyber-attacks Ally could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it. . . .

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

[7] *Id.* at 3-4.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[8]

38. To prevent and detect cyber-attacks or ransomware attacks Ally could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

[8] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Sept. 4, 2024).

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[9]

39. Given that Ally was storing the sensitive PII of Plaintiffs and Class Members, Ally could and should have implemented all of the above measures to prevent and detect cyberattacks.

40. The occurrence of the Data Breach indicates that Ally failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of allegedly billions of individuals, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, and Stores Plaintiffs' and the Class's PII.

41. As part of its business, Ally acquires the sensitive PII of its customers, including Plaintiffs and Class Members.

42. Defendant retains and stores this information and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiffs' and Class Members' PII, Ally would be unable to perform its services.

43. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Ally assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

44. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Ally to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

[9] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Sept. 4, 2024).

45. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members.

46. Upon information and belief, Ally made promises to its clients and thereby Plaintiffs and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

47. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew, or Should Have Known, of the Risk Because Financing Companies in Possession of PII are Particularly Susceptible to Cyber Attacks.

48. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and other sensitive information, like Ally, preceding the date of the breach.

49. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Ally knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

50. Data thieves regularly target companies like Ally's due to the highly sensitive information in their custody. Ally knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

51. Indeed, cyber-attacks, such as the one experienced by Ally, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a

warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[10]

52. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[11]

53. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[12]

54. Despite the prevalence of public announcements of data breach and data security compromises, Ally failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

55. Additionally, as companies became more dependent on computer systems to run their business,[13] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[14]

56. As a custodian of PII, Ally knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class members, and of the foreseeable

---

[10] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited Sept. 4, 2024).

[11] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6 (last visited Sept. 4, 2024).

[12] *Id*.

[13] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited Sept. 4, 2024).

[14] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited Sept. 4, 2024).

consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

57. At all relevant times, Ally knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Ally's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

58. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Ally's server(s), amounting to potentially billions of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

59. To make matters worse, Ally has not even provided any notice to any of the affected individuals whose PII was stolen in the Data Breach. This total failure to notice and a failure to compensate Plaintiffs and Class Members. Moreover, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services in order to protect themselves from the consequences of Ally's actions.

60. The injuries to Plaintiffs and Class Members were directly and proximately caused by Ally's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

61. The ramifications of Ally's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

62. As a background search company in possession of individuals' sensitive PII, Ally knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiffs

and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Ally failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifying Information

63. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

64. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[17] For example, Personal Information can be sold at a price ranging from $40 to $200.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

65. For example, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to

[15] 17 C.F.R. § 248.201 (2013).
[16] *Id.*
[17] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Sept. 4, 2024).
[18] *Here's How Much Your Personal Information Is Selling for on the dark web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Sept. 4, 2024).
[19] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Sept. 4, 2024).

change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[20]

66. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

67. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

68. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information

[20] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 4, 2024).
[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Sept. 4, 2024).

compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

69. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[22]

70. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

71. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

72. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

Defendant Fails to Comply with FTC Guidelines.

---

[22] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sept. 4, 2024).

[23] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Sept. 4, 2024).

73. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

74. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[24]

75. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[25]

76. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

77. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

[24] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Sept. 4, 2024).
[25] *Id.*

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

78. These FTC enforcement actions include actions against financial companies, like Ally. *See, e.g., In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 408 (E.D. Va. 2020) (*"*Plaintiffs have plausibly alleged a claim" based upon violation of Section 5 of the FTC Act.)

79. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Ally, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Ally's duty in this regard.

80. Defendant failed to properly implement basic data security practices.

81. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

82. Upon information and belief, Ally was at all times fully aware of its obligation to protect the PII of Plaintiffs and Class Members, Ally was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Ally's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Fails to Comply with Industry Standards.

83. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

84. Several best practices have been identified that, at a minimum, should be implemented by financial companies in possession of PII, like Ally, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Ally failed to follow these industry best practices, including a failure to implement multi-factor authentication.

85. Other best cybersecurity practices that are standard in Ally's industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Ally failed to follow these cybersecurity best practices, including failure to train staff.

86. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

87. These frameworks are existing and applicable industry standards in Ally's industry, and upon information and belief, Ally failed to comply with at least one—or all—of these accepted standards, opening the door to the threat actors and causing the Data Breach.

Common Injuries and Damages

88. As a result of Ally's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession of Ally, and which is subject to further breaches, so long as Ally fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

Data Breaches Increase Victims' Risk of Identity Theft.

89. The unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers. Indeed, at least one of the Plaintiffs has already been alerted that their PII has been found on the dark web.

90. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Simply, unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

91. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the

data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

92. Plaintiffs' and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

93. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

94. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

95. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[26]

26Fullz is slang for "an information package containing a person's real name, address, and form of ID, or their "full information." Fullz can be considered a component of 3rd party fraud, as the person whose credentials are sold is not complicit. Fraudsters use these credentials to steal identities and commit financial fraud. Fullz usually contains a person's name, address, SSN, driver's license, bank account credentials, and medical records, among other details. Fraudsters use the victim's financial reputation for identity theft and fraud, resulting in low credit scores and financial insecurity for the victims. For example, they apply for a loan or credit card with the victim's good credit. The fraudster applies for the card and uses it, while the victim cannot pay it

96. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

97. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

98. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the Data Breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

99. Thus, even if certain information (such as telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

100. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

101. As a result of the recognized risk of identity theft, when a Data Breach occurs, and assuming an individual is notified by a company that their PII was compromised, which Ally has

off and/or attempts to cancel it, harming their credit score." https://fraud.net/d/fullz/ (last accessed on November 13, 2024).

failed to do in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

102. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

103. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as monitoring their credit and reviewing their financial accounts for any indication of fraudulent activity, which may take years to detect.

104. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[27]

105. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[28]

---

[27] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited Sept. 4, 2024).

[28] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Sept. 4, 2024).

106. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[29]

Diminution Of Value Of PII

107. PII is a valuable property right.[30] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

108. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[31]

109. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[32] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[33,34]

---

[29] https://www.gao.gov/assets/a262904.html (last visited November 13, 2024).
[30] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sept. 4, 2024) ("GAO Report").
[31] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[32] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sept. 4, 2024).
[33] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Sept. 4, 2024)
[34] https://datacoup.com/ (last visited Sept. 4, 2024).

110. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available on the dark web, and the rarity of the Data has been lost, thereby causing additional loss of value.

111. At all relevant times, Ally knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Ally's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

112. Fraudulent activity perpetrated against Plaintiffs and the Class Members that will result from the Data Breach may not come to light for years.

113. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

114. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Ally's network, amounting to potentially billions of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

115. The injuries to Plaintiffs and Class Members were directly and proximately caused by Ally's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary.

116. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes, *e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

117. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their PII was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

118. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

119. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Ally's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Ally's failure to safeguard their PII.

Loss Of Benefit Of The Bargain

120. Furthermore, Ally's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. Upon information and belief, when agreeing to pay Ally for its banking services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the PII, when in fact, Ally did

not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Ally.

PLAINTIFFS' EXPERIENCES

Plaintiff Owens

121. Plaintiff Sebestian Owens has had checking and savings accounts with Ally since 2017.

122. Plaintiff's PII, including but not limited to, his Social Security number, was in the possession, custody and/or control of Ally at the time of the Data Breach.

123. Plaintiff believed that Ally would take, at a minimum, industry standard precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure, and would timely notify him of any data security incidents related to her. Plaintiff would not have given his PII to Ally had he known it would not take reasonable steps to safeguard his PII.

124. As a result of the Data Breach, Plaintiff has or will make reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or personal records for any indications of actual or attempted identity theft or fraud.

125. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Ally obtained from Plaintiff; (b) violation of his privacy rights; (c) the theft of his PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

126. In addition, he already noticed an incorrect item on his credit report following the

Data Breach, involving an auto loan he did not take out, causing his credit score to precipitously drop.

127. As a result of the Data Breach, Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

128. The Data Breach has caused Plaintiff to suffer significant anxiety and stress, which has been compounded by the fact that his Social Security number and other intimate details are in the hands of criminals and being sold on the dark web.

129. As a result of the Data Breach, Plaintiff anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for his lifetime.

130. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Ally's possession, is protected and safeguarded from future breaches.

Plaintiff Hamilton

131. Plaintiff is a former customer of Defendant, whose services he used to finance two of his vehicles.

132. As Defendant's customer, Plaintiff was required to provide his Private Information, including his Social Security number, to Defendant, as part of their banking relationship.

133. Plaintiff is not aware of any data breaches other than this one that exposed his Private Information and is concerned that it and other Private Information has now been exposed to bad actors.

134. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the

value of Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

135. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

136. Plaintiff greatly values his privacy, and would not have provided his Private Information, undertaken the services and paid the amounts that he did if he had known that his Private Information would be maintained using inadequate data security systems.

Plaintiff Craig

137. Plaintiff Craig is a consumer who has a bank account through Ally. Ally required that Plaintiff Craig provide it with his PII. Ally was provided with his personal information, including but not limited to his Social Security number.

138. Around or after January 29, 2024, Plaintiff Craig received the Notice of Data Breach letter, which indicated that Ally had known about the Data Breach for over a month. The letter informed him that his critical PII was accessed by an unauthorized actor. The letter stated that the extracted information included his "name, address, Social Security number, loan number, and financial account number" but did not expand on whether additional information was stolen as well.

139. Plaintiff Craig is alarmed by the amount of his Personal Information that was stolen or accessed, and even more by the fact that his Social Security number was identified as among the breach data on Ally's computer system.

140. Since the Data Breach, Plaintiff Craig has been notified that his Social Security number, date of birth and address has been found on the dark web. Plaintiff also found that someone froze his credit other than him. Given the time frame, he believes these incidents are related to the Data Breach.

141. In response to Ally's Notice of Data Breach, Plaintiff will be required to spend time dealing with the consequences of the Data Breach, which will continue to include time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts.

142. Immediately after receiving the Notice Letter, Plaintiff changed his passwords and started to check his financial accounts for an hour or more per week in an effort to mitigate the damage that has been caused by Ally.

143. Plaintiff is very careful about sharing PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

144. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided Ally with his PII had Ally disclosed that it lacked data security practices adequate to safeguard PII.

145. Plaintiff suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that they entrusted to Ally.

146. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

147. Plaintiff Craig reasonably believes that his Private Information may have already been sold by cybercriminals. Had he been notified of Ally's breach in a more timely manner, he could have attempted to mitigate his injuries.

148. Plaintiff Craig has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

149. Plaintiff has a continuing interest in ensuring that his PII, which upon information and belief remains backed up and in Ally's possession, is protected and safeguarded from future breaches.

V. CLASS ACTION ALLEGATIONS

150. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

151. The Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the Data Breach (the "Class").

152. Excluded from the Class are the following individuals and/or entities: Ally and Ally's parents, subsidiaries, affiliates, officers and directors, and any entity in which Ally have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

153. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

154. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. On information and belief potentially billions of individuals will soon be notified by Ally of the Breach. The Class is apparently identifiable within Ally's records, and Ally has already identified these individuals or is in the process of doing so (as evidenced by sending them breach notification letters).

155. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class Members, including the following:

a. Whether and to what extent Ally had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Ally had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Ally had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Ally failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Ally actually learned of the Data Breach;

f. Whether Ally adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Ally violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Ally failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Ally adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Ally's wrongful conduct;

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

156. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

157. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

158. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will

permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Ally. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

159. The litigation of the claims brought herein is manageable. Ally's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

160. Adequate notice can be given to Class Members directly using information maintained in Ally's records.

161. Unless a Class-wide injunction is issued, Ally may continue in its failure to properly secure the PII of Class Members, Ally may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Ally may continue to act unlawfully as set forth in this Complaint.

162. Further, Ally has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

163. Plaintiffs repeat and re-allege the preceding paragraphs in the Complaint as if fully set forth herein.

164. Upon information and belief, Plaintiffs and Class Members entrusted Ally with their PII as a condition of obtaining financial services.

165. Ally owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

166. Ally had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

167. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Ally and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Avfue with their confidential PII.

168. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Ally is bound by industry standards to protect confidential PII.

169. Ally was subject to an "independent duty," untethered to any contract between Ally and Plaintiffs or the Class.

170. Ally also had a duty to exercise appropriate clearinghouse practices to remove individuals' PII it was no longer required to retain pursuant to regulations.

171. Ally also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Class.

172. Ally breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Ally include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised;

f. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

173. Ally violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Ally's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

174. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

175. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

176. Defendant's violation of the FTC Act is prima facie evidence of negligence.

177. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

178. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Ally's inadequate security practices.

179. It was foreseeable that Ally's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

180. Ally has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

181. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Ally knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Ally's systems.

182. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

183. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Ally's possession.

184. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

185. Ally had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Ally's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

186. But for Ally's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

187. There is a close causal connection between Ally's failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Ally's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

188. As a direct and proximate result of Ally's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Ally's possession and is subject to further unauthorized disclosures so long as Ally fails to undertake appropriate and adequate measures to protect the PII.

189. As a direct and proximate result of Ally's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

190. Additionally, as a direct and proximate result of Ally's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Ally's possession and is subject to further unauthorized disclosures so long as Ally fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

191. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

192. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

193. Plaintiffs and Class Members are also entitled to injunctive relief requiring Ally to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

194. Plaintiffs repeat and re-allege the preceding paragraphs in the Complaint as if fully set forth herein.

195. When Plaintiffs and Class Members provided their PII to Ally, Plaintiffs and Class Members entered into implied contracts with Ally pursuant to which Ally agreed to safeguard and protect such PII and to timely and accurately notify Plaintiffs and Class Members that their PII had been breached and compromised.

196. Ally required Plaintiffs and Class Members to provide and entrust their PII as a condition of obtaining financial services.

197. Plaintiffs and Class Members would not have provided and entrusted their PII to Ally in the absence of the implied contract between them and Ally.

198. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Ally.

199. Ally breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect the PII of Plaintiffs and Class Members.

200. As a direct and proximate result of Ally's breach of the implied contracts, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

201. Plaintiffs repeat and re-allege the preceding paragraphs in the Complaint as if fully set forth herein.

202. This count is pleaded in the alternative to the breach of implied contract count above (Count II).

203. Plaintiffs and Class Members conferred a monetary benefit to Ally when they provided their PII to Ally.

204. Defendant knew that Plaintiffs and Class Members conferred a monetary benefit to it, and it accepted and retained that benefit. Ally profited from this monetary benefit, as the transmission of Plaintiffs' and Class Members' PII to Ally from its clients is an integral part of

Ally's business. Without collecting and maintaining Plaintiffs' and Class Members' PII, Ally would be unable to conduct its business.

205. Defendant was supposed to use some of the monetary benefit provided to it by its clients at Plaintiffs' and Class Members' expense to secure the PII belonging to Plaintiffs and Class Members by paying for costs of adequate data management and security.

206. Defendant should not be permitted to retain any monetary benefit belonging to Plaintiffs and Class Members because Ally failed to implement necessary security measures to protect the PII of Plaintiffs and Class Members.

207. Defendant gained access to the Plaintiffs' and Class Members' PII through inequitable means because Ally failed to disclose that it used inadequate security measures.

208. Plaintiffs and Class Members were unaware of the inadequate security measures and would not have entrusted their PII to Ally's clients, and thereby Ally, had they known of the inadequate security measures.

209. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiffs and Class Members have no adequate remedy at law.

210. As a direct and proximate result of Ally's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Ally's possession and is subject to further unauthorized disclosures so long as Ally fails to undertake appropriate and adequate measures to protect the PII.

211. As a direct and proximate result of Ally's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

212. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds from the monetary benefit that it unjustly received from them.

COUNT IV
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

213. Plaintiffs repeat and re-allege the preceding paragraphs in the Complaint as if fully set forth herein.

214. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

215. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether Ally is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs alleges that Ally's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in future.

216. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Ally owes a legal duty to secure customers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTCA; and

b. Ally continues to breach this legal duty by failing to employ reasonable measures to secure its customers' PII.

217. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Ally. The risk of another such breach is real, immediate, and substantial. If another breach at Ally occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and he will be forced to bring multiple lawsuits to rectify the same conduct.

218. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Ally if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Ally of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Ally has a pre-existing legal obligation to employ such measures.

219. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Ally, thus eliminating the additional injuries that would result to Plaintiffs and other individuals whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

A. Plaintiffs, individually and on behalf of all other members of the class, respectfully request that the Court enter judgment in Plaintiffs' favor and against Ally as follows:

B. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

C. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, nominal damages and disgorgement;

D. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the class, seek appropriate injunctive relief designed to prevent Ally from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

E. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

G. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: November 20, 2024

Respectfully submitted,

/s/ Joel R. Rhine
Joel R. Rhine
Rhine Law Firm, P.C.
N.C. Bar: 16028
jrr@rhinelawfirm.com
Ruth A. Sheehan
N.C. Bar: 48069
ras@rhinelawfirm.com
1612 Military Cutoff, Suite 300
Wilmington, North Carolina 28403
Telephone: 910-772-9960

Fax: 910-772-9062

s/ David M. Wilkerson
David M. Wilkerson
NC State Bar No. 35742
Attorney for Plaintiff
The Van Winkle Law Firm
11 N. Market Street
Asheville, North Carolina 28801
(828)258-299 (phone)
(828)257-2767 (fax)
dwilkerson@vwlawfirm.com

Danielle L. Perry*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
Email: gmason@masonllp.com
Email: dperry@masonllp.com
Email: lwhite@masonllp.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
ostrow@kolawyers.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Attorneys for Plaintiffs

**Admitted pro hac vice*